



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/099,735 | 03/15/2002 | James H. Price | 1348-1013 | 4217 |

32376 7590 03/01/2006

LAWRENCE R. YOUST
DANAMRAJ & YOUST, P.C.
5910 NORTH CENTRAL EXPRESSWAY
SUITE 1450
DALLAS, TX 75206

EXAMINER

GEE, JASON KAI YIN

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 03/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|-------------------------------|------------------------------|--|
| Office Action Summary | Application No. 10/099,735 | Applicant(s) PRICE ET AL. | |
| | Examiner Jason K. Gee | Art Unit 2134 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03/15/2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 March 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is response to communication: filed on 03/15/2002.
2. Claims 1-18 are currently pending in this application. Claims 1, 10, and 15 are independent claims.
3. No IDS was received for this application.

Specification

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "System and Method for Automatically Configuring a Client Device with a User Key Set".

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 10-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 10-14, claim 10 recites 'a registration server' more than once. It is unclear whether the recited registration servers are the same server or if they are different embodiments.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Independent claim 15 is rejected under 35 U.S.C. 102(e) as being anticipated by Jerdonek US Patent Application Publication 2002/0095569 (hereinafter '569).

As per independent claim 15, '569 teaches a client device ('key wallet' paragraphs 39-40) installed in a data network access device (client systems, Figure 1, systems 130, 140, 150). Routers are taught in paragraph 23 and the IP protocol is used, as indicated in paragraph 26. The network access device includes the router, as Figure 1 and paragraph 23 display and describe the client devices connecting to the routers. The network devices as indicated in paragraph 26 can utilize the Internet Protocol, which indicates the system can route IP signals from different networks. The clients can connect to a network with a plurality of users connected to the network access device, as the clients can connect to a local area network or an intranet. Means for storing a preprogrammed common key set is taught in paragraph 39. Means for requesting access to the remote data network utilizing the preprogrammed common key set for authentication purposes when the client device is installed in the network access

device is taught in paragraph 44. Means for receiving a new user key set from the network is taught in paragraphs 47-48. These paragraphs along with paragraphs 49-53 indicate that the common key set is replaced with the new key set, as the new key set is used to connect to the remote server. Means responsive to receiving the new user key set for automatically requesting access to the remote data network utilizing the new user key set for authentication purposes is also taught in paragraphs 47-48, and paragraph 61 teaches that it may be automatic.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek ('569), and further in view of William Stallings' *Cryptography and Network Security – Principles and Practice*, Second Edition (1999).

As per independent claim 1, '569 teaches a method of automatically configuring and authenticating a client device('key wallet' paragraphs 39-40) installed in a data network access device (client systems, Figure 1, systems 130, 140, 150). Routers are taught in paragraph 23 and the IP protocol can be used, as indicated in paragraph 26.

The network access device includes the router, as Figure 1 and paragraph 23 display and describe the client devices connecting to the routers. The network devices as indicated in paragraph 26 can utilize the Internet Protocol, which indicates the system can route IP signals from different networks. The clients can connect to a network with a plurality of users connected to the network access device, as the clients can connect to a local area network or an intranet. Paragraph 39 teaches that a user has a preprogrammed common key set. Requesting access to the remote data network by the client device using the preprogrammed common key set for authentication purposes is taught in paragraph 44. Paragraph 45-46 then goes on to teach that the client is directed to a registration server (authentication server 350) after it is authenticated (the common key set is valid). The registration server is accessed, and the client receives a new user key set (paragraphs 47-48). Requesting access to the remote data network by the client device using the new user key set for authentication purposes is taught in paragraphs 49 and 50. The client device has then full network access upon determining that the new user key set is valid (paragraph 60). Paragraph 61 also teaches that all these steps may be automatic.

However, '569 does not explicitly teach that an authenticator can both determine whether the common key set is valid and also determining whether the new user key set is valid. In '569, the 'external server' 310 authenticates both the common key set and the new user key set. '569 teaches the use of an SSL connection from the client to the server in paragraph 45, but does not teach the specifics of it. The specifics of SSL can be taught by Stallings. With an SSL connection, a client and his key are authenticated

by a server, as indicated on pages 454 and 455. In this way, the 'external server' in '569 is an authenticator of the common key set, as the client connects to this the external server using SSL. Also, the external server authenticates the second key set, as it receives the digital signature of the new key set through a secure communications line such as SSL described in '569 paragraphs 59-53.

At the time of the invention, it would have been obvious to combine '569 with Stallings to include that a server authenticates a client in an SSL connection. One of ordinary skill in the art would have been motivated to perform such an addition as mutual authentication is a standard for SSL. The specifics of SSL can be found on pages 451 to page 455 of Stalling's book.

As per claim 2, the step of requesting access to the remote data network by the client device using the common key set for authentication purposes includes automatically requesting access to the remote data network by the client device using the common key set for authentication purposes (paragraph 61 of '569).

As per claim 3, paragraph 46 of '569 teaches that the registration server is associated with the common key set in an authentication database. Providing the client device with limited network access includes providing the client device with access only to a registration server is already rejected in claim 1. The registration server is associated with the common key set, as the registration server cannot be accessed until the common key set is used or accessed, as can be seen in the steps leading up to accessing the registration server.

As per claim 4, paragraph 61 of '569 indicates that the registration server can automatically assign the new user key set. Sending the new user key set from the registration server to the client device is already rejected in claim 1.

As per claim 5, paragraphs 47-48 of '569 teaches that a new user key is sent from the registration server (authentication server 350) to an authenticator (external server 310).

As per claim 6, paragraphs 47-48 of '569 teaches that a new user key set is sent from the authenticator to the client device. As rejected in claim 1, the authenticator is the external server.

As per claim 7, the user selects the new user key set as the user requests a key and obtains it from the authentication server 350, as described in '569 lines 45-48.

As per claim 8, paragraphs 47-48 of '569 teaches that the new user key is sent from the registration server (authentication server 350) to an authenticator (external server 310). These paragraphs also teach that the key is sent from the authenticator to the client device.

Independent claim 10 is rejected using the same basis of arguments used to reject claim 1, as claim 10 is directed to an apparatus. '569 teaches the means for the apparatus.

10. Claims 9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Ketcham US Patent No. 6,075,860 (hereinafter '860).

As per claim 9, '569 and Stallings teaches all the limitations of claim 1. Receiving a new user key set and automatically requesting access to the remote data network by the client device using a new user key set is already rejected in the arguments for claim 1. However, authenticating by the client device that the new user key set is received from a valid source is not taught in '569. Validating sources in which a user is connecting to is taught in '860 though, where a client device authenticates that the source in which it connects to is a valid source (col. 10 lines 10-37).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include validating a source in which a user is connecting to. One of ordinary skill in the art would have been motivated to perform such an addition to create a mutual authentication channel in order for communication to be secure bidirectionally: "Furthermore, there exists a need for providing a method and system for establishing an encrypted authenticated wireless communication channel between an authorized user and a computer network."

Claim 12 is rejected using the same basis of arguments used to reject claim 9.

11. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Walker et al. US Patent Application Publication No. 2003/0037250 (hereinafter '250).

As per claim 11, '569 and Stallings teaches all the limitations of claim 10, but does not teach an authentication database that associates a plurality of common key

sets with a plurality of registration servers. However, '250 teaches a database associating keys with the respective servers (paragraph 17).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine an authentication system with an authentication database comprising of keys associated with their servers. One of ordinary skill in the art would have been motivated to perform such an addition to provide a secured access controller capable of communicating with a plurality of content servers: "It is a primary object of the present invention to provide a secured access controller for use in connection with a network capable of communicating with a plurality of content servers that store content objects and a plurality of client processing systems capable of requesting access to the stored content objects" (paragraph 17).

12. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Heller US Patent Application Publication No. 2002/0101857 (hereinafter '857).

As per claim 13, '857 teaches a user utilizing PPP for signaling with other devices. Paragraphs 19 and 20 summarize this. It is also discussed in paragraph 35 that this method is used to connect a user to a server.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the use of PPP for a client to signal systems in an authentication system and method. One of ordinary skill in the art would have been motivated to perform such an addition to improve the method and system for communicating information between a source and a destination using PPP: "Therefore, there is a

general need in the art for an improved method and system for communicating information between a source and a destination using PPP. In particular, there is a need in the art for a method and system for communicating PPP packets between a source and a destination without the need for reconnection if the source is mobile” (paragraph 18).

As per claim 14, a client device is installed in a CPE comprising a DSL modem ('857 paragraph 14). Paragraph 27 of '857 teaches an IP router.

13. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 as applied above, and further in view of '860.

As per claim 16, '569 teaches all the limitations of claim 15. However, authenticating by the client device that the new user key set is received from a valid source is not taught in '569. Validating sources in which a user is connecting to is taught in '860 though, where a client device authenticates that the source in which it connects to is a valid source (col. 10 lines 10-37).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include validating a source in which a user is connecting to. One of ordinary skill in the art would have been motivated to perform such an addition to create a mutual authentication channel in order for communication to be secure bidirectionally:
“Furthermore, there exists a need for providing a method and system for establishing an encrypted authenticated wireless communication channel between an authorized user and a computer network.”

14. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 as applied above, and further in view of '857.

As per claim 17, '857 teaches a user utilizing PPP for signaling with other devices. Paragraphs 19 and 20 summarize this. It is also discussed in paragraph 35 that this method is used to connect a user to a server.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the use of PPP for a client to signal systems in an authentication system and method. One of ordinary skill in the art would have been motivated to perform such an addition to improve the method and system for communicating information between a source and a destination using PPP: "Therefore, there is a general need in the art for an improved method and system for communicating information between a source and a destination using PPP. In particular, there is a need in the art for a method and system for communicating PPP packets between a source and a destination without the need for reconnection if the source is mobile" (paragraph 18).

As per claim 18, a client device is installed in a CPE comprising a DSL modem ('857 paragraph 14). Paragraph 27 of '857 teaches an IP router.

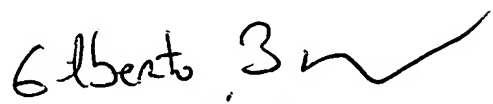
Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
02/20/06


GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

ECT